ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 9/25 (September)

Insights from Ensign Cyber Threat Landscape Report 2025

INTRODUCTION

1. Amidst intensifying geopolitical tensions, trade disputes, and persistent economic uncertainty, cyber threat activity has escalated in both scale and sophistication. These macro-level disruptions have catalysed the operations of threat actors, who increasingly leverage the Underground Economy to enhance their capabilities and expand their reach.

2. The Ensign Cyber Threat Landscape Report 2025 offers a strategic overview of key developments observed in 2024 and provides forward-looking insights into how cyber threats may evolve in 2025 and beyond. The report highlights several critical trends:

- **Institutionalisation of the Underground Economy**: Threat actors are engaging in more structured and collaborative interactions within illicit digital markets. This has led to a measurable increase in the effectiveness and success rates of cyber-attacks, as actors pool resources and specialise in distinct operational roles.

- **Significance of Mastermind Threat Groups**: A growing number of threat actors are aligning themselves with larger, more coordinated entities – referred to as “mastermind groups.” This convergence blurs traditional distinctions between cybercriminals, hacktivists, and state proxies, complicating attribution and legal responses. The ambiguity surrounding their identities poses challenges for defenders and policymakers alike.

- **Technological Fragmentation and Supply Chain Vulnerabilities**: The diversification of technology stacks and ongoing transitions in global supply chains have introduced new vectors of vulnerability. These systemic shifts strain the capacity of defenders to respond swiftly and effectively, particularly in environments where legacy systems coexist with emerging technologies.

INSTITUTIONALISATION OF THE UNDERGROUND ECONOMY

3. Recent developments in the cyber threat landscape reveal a thriving Underground Economy and a marked increase in the operational sophistication of threat actors. These trends carry significant implications for national security, digital sovereignty, and the governance of cyberspace.

a. Lowered Barriers to Entry for Ransomware Operations. The public leak of operational playbooks and source code from prominent ransomware groups such as LockBit Gang and Conti has democratised access to advanced cyber-attack methodologies. This has enabled the rapid emergence of opportunistic and transient ransomware collectives – such as Hunters International and RansomHub – which, despite lacking long-term strategic intent, can execute disruptive attacks with minimal setup.

b. Convergence of Hacktivist and Organised Crime Groups. There is growing evidence that hacktivists are increasingly pivoting to cybercrime because of the higher availability of or ease of access to tooling in underground forums or repositories. This results in both the blurring of lines between Hacktivist groups and Organised Crime Groups and the cross-pollination of tactics, tools, and operational knowledge. Notable among these is the widespread use of Bring Your Own Vulnerable Driver (BYOVD) modules – such as *EDRKillShifter*, *AvNeutralizer*, and *AuKill* – designed to disable endpoint detection systems. Additionally, Living off the Land (LOTL) techniques, which exploit native system utilities for stealthy lateral movement, are increasingly employed to evade detection and prolong access.

c. <u>Rise of Specialisation and Cooperative Campaigns</u>. Cyber-attack campaigns now frequently involve subcontracting and specialisation, mirroring the structure of legitimate industries. Threat groups leverage:

- **Initial Access Brokers** to infiltrate target networks;
- **Ransomware-as-a-Service (RaaS) Operators** to manage extortion and payments; and
- **Exploit Developers** to craft bespoke attack tools.

This modular approach enhances scalability and success rates, allowing threat actors to target a broader range of victims with greater precision and efficiency.

4. These developments underscore the need to reassess the frameworks governing cyber conflict. The increasing professionalisation and decentralisation of cybercrime challenge traditional notions of attribution, deterrence, and legal accountability. Moreover, the blurred boundaries between ideological and criminal actors complicate efforts to regulate and respond to cyber threats within existing international norms.

SIGNIFICANCE OF MASTERMIND THREAT GROUPS

5. The rise of Mastermind Threat Groups, encompassing both Organised Crime Groups and State-Sponsored Threat Groups, has reshaped the operational dynamics of cyber conflict. These entities increasingly outsource discrete components of their campaigns to specialised actors within the Underground Economy, creating a decentralised yet highly coordinated threat ecosystem.

6. This fragmentation of roles has led to the emergence of niche capabilities, including:

- **Initial Access Brokers**, who provide compromised entry points into targeted systems;
- **Payment and Laundering Specialists**, responsible for obfuscating and converting illicit financial gains;
- **Negotiators and Victim Support Operators**, who manage extortion communications and facilitate ransom payments;

- **Ransomware-as-a-Service (RaaS) Operators**, who maintain leak sites and orchestrate ransomware deployments; and
- **Exploit Developers**, who engineer bespoke tools and platforms to enable sophisticated attacks.

7. Such specialisation enhances operational efficiency and success rates, allowing Mastermind Threat Groups to scale their campaigns while maintaining plausible deniability. In some cases, auxiliary actors are deployed not for primary attack execution but to distract and exhaust the victim's resources, enabling the core group to operate with reduced resistance.

8. The convergence of Hacktivist groups with Organised Crime Groups further complicates attribution and response. When ideological actors collaborate with profit-driven entities, their identities blur, and their capabilities are amplified – often necessitating their reclassification as criminal actors. A case in point is the evolution of DragonForce Malaysia, a former hacktivist collective, into the DragonForce Ransomware Group, now operating with the structure and intent of an organised crime group. While this transformation has increased their operational effectiveness, it has also rendered them more predictable and thus more vulnerable to defensive profiling.

9. The use of proxy actors by State-Sponsored Threat Groups introduces further complexity. By engaging criminal or hacktivist entities, states can conduct cyber operations below the threshold of armed conflict, thereby avoiding direct attribution and escalation. However, this tactic entangles non-state actors in state-driven campaigns, raising profound questions about legal accountability, norm development, and international cyber governance.

10. The evolving threat landscape underscores the need to reexamine traditional frameworks of conflict, sovereignty, and criminality in cyberspace. The blurred lines between state and non-state actors, ideological and financial motives, and overt and covert operations demand a recalibration of both domestic and international responses to cyber threats.

TECHNOLOGICAL FRAGMENTATION AND SUPPLY CHAIN VULNERABILITIES

11. The ASEAN region presents a complex and evolving technological landscape, characterised by the coexistence of mature Western systems, rapidly advancing Eastern innovations, and the widespread adoption of open-source platforms. This diversification, while fostering innovation and strategic autonomy, also introduces multifaceted vulnerabilities across both technological and human dimensions.

12. At the technological level, organisations are grappling with persistent operational challenges in securing mature Western technologies – systems that, despite their familiarity, are increasingly susceptible to sophisticated threats. The integration of emerging Eastern technologies further compounds these challenges, as these systems often embody distinct security paradigms and defence architectures, making harmonisation within existing infrastructures particularly arduous.

13. Moreover, the proliferation of open-source technologies – while democratising access and accelerating development – has become a focal point for threat actors. The deliberate targeting and compromise of open-source libraries underscore the urgency for robust vulnerability management frameworks and proactive threat intelligence.

14. On the human front, the heterogeneous nature of the technology stack demands a highly skilled and adaptable cybersecurity workforce. Defenders must possess cross-domain expertise to effectively mitigate risks inherent in diverse systems. However, this requirement is exacerbated by a regional scarcity of cybersecurity talent and intense competition for skilled professionals, placing additional strain on institutional capacity to safeguard digital assets.

15. ASEAN's technological pluralism, while strategically significant, necessitates a recalibration of both policy and operational approaches to cybersecurity – balancing innovation with resilience in an increasingly contested digital domain.

16. Arising from the trade tensions, organisations are also increasingly implementing business strategies for near-shoring and reshoring, causing the cyber supply chains to be redrawn. The transitions from established suppliers to

new providers will expose organisations to cyber supply chain risks which can compromise the organisation and their connected parts.

FORECASTING BEYOND 2025

17. The Ensign Cyber Threat Landscape Report 2025 builds upon critical observations from 2024 to forecast emerging dynamics in the global cyber threat environment. Against the backdrop of intensifying geopolitical rivalries, economic instability, and technological disruption, the report outlines five key trends likely to shape cyber risk in 2025 and beyond:

a. Ransomware Consolidation and Tactical Evolution. Ransomware continues to function as a persistent digital threat – akin to an "endemic digital flu." The leak of source code and operational playbooks from major Ransomware groups has significantly lowered the barriers to entry, enabling opportunistic actors to replicate and modify attack frameworks for financial gain. This proliferation is driving both experimentation and consolidation, resulting in increasingly sophisticated and resilient Ransomware operations.

b. State-Sponsored Threat Groups Pre-Positioning for Strategic Leverage. In an era where information dominance is central to geopolitical negotiations, state-sponsored threat groups are intensifying cyber espionage campaigns. These actors are not only gathering intelligence but also deploying targeted disruptions to exert pressure during diplomatic or trade negotiations. The systemic implications of such operations are amplified by complex technology integrations and global supply chain interdependencies, making attribution and response more difficult.

c. Rising Incident Frequency Amid Technological Complexity. As organisations accelerate digital transformation – particularly through the adoption of AI technologies – they face mounting challenges in asset visibility, vulnerability management, and patching latency. The growing gap between vulnerability discovery and remediation is contributing to a surge in exploit activity, increasing the cumulative "patching debt" and exposing critical infrastructure to sustained risk.

d. Cyber Supply Chain Vulnerabilities Amid Strategic Realignment. Trade tensions and geopolitical decoupling/derisking are prompting organisations to restructure their supply chains, including digital dependencies. This transition phase introduces heightened exposure to cyber supply chain compromises, as legacy systems are replaced or reconfigured without adequate security oversight. The redrawing of supplier relationships creates new attack surfaces and transitional risks.

e. AI Adoption Outpaces Security Governance. The rapid deployment of AI technologies across sectors is outstripping the development of corresponding security controls. Organisations are experimenting with AI use cases that require broad access to sensitive data repositories, often without adequate safeguards. This misalignment between innovation and governance is creating a "control gap," increasing the likelihood of data leaks and privacy breaches. Traditional data security frameworks may lack the flexibility to balance AI utility with risk mitigation.

18. These evolving trends in the cyber threat landscape underscore the imperative for deeper strategic engagement at the intersection of technology, statecraft, and transnational criminal activity. The increasing complexity and interdependence of digital systems demand a recalibration of international norms, legal frameworks, and deterrence strategies to safeguard digital sovereignty and uphold global stability. Furthermore, they highlight the urgent need for collective defence models – both at the intergovernmental and inter-organisational levels – to effectively address the multifaceted challenges posed by cyber threats in an era of geopolitical fragmentation and technological acceleration.

DEFENSIVE ACTIONS FOR CYBER DEFENDERS & LEADERS

19. Finally, we identified the essential defensive measures and detection data sources that organisations can adopt to mitigate risks in Initial Access, Command and Control, Exfiltration, and Impact tactics as outlined in the MITRE ATT&CK framework.

20. The thematic defence strategies highlighted below centres on the crucial necessity for consistent monitoring across the digital attack surface and

integrating cyber threat intelligence analysis to embrace a threat-informed approach, especially in responding to impending and material threats.

i. Ensure that KRIs are tied to threats and mapped to security monitoring measurements.
ii. Rehearse, drill and practice all incident-to-crisis processes to build up readiness and resilience in cyber defence.
iii. Adopt the 3-2-1-1 backup, archival and recovery strategy.
iv. Enhance Asset Inventory and Monitoring Coverage, Leveraging Threat Intelligence.
v. Review and harden configurations of systems and platforms, including key user interaction interfaces.
vi. Integrate incident response plans to crisis management plans, ensuring whole-of-organisation coordination

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

. . . . .